METHODS OF AUTHENTICATING A USER

CROSS-REFERENCE TO RELATED APPLICATION

[0001] This application is a continuation of U.S. patent application Ser. No. 14/022,104, filed Sep. 9, 2013, and entitled "Use of a Biometric Image in Online Commerce," the contents of which are incorporated herein by reference as if fully disclosed herein.

TECHNICAL FIELD

[0002] The present invention relates to electronic devices, and more particularly to a biometric sensing device included in, or connected to an electronic device. Still more particularly, the present invention relates to the use of one or more biometric data in online commerce.

BACKGROUND

[0003] Passwords are a common security tool for applications, websites, and devices. A user-entered password must match a reference password before the user is given access or allowed to interact with an application, website, or device. But passwords can have a number of limitations. The number of characters that can be included in the password can be limited to a maximum number, such as eight or twelve characters. Additionally, a user can be prohibited from using certain types of characters in their password. For example, a password may not include symbols such as a pound or hash symbol (#), an exclamation sign (!), and a percent sign (%). Randomly generated passwords can be more secure than passwords that are selected by a user, but randomly generated passwords can be difficult to remember. Some users therefore prefer to select passwords that are easier to remember at the expense of security. For example, a password that includes a complete word, the user's birthday, or a company name may be easier to remember, but such passwords can also be easier to guess or discover.

[0004] The use of biometric data can provide a greater level of security to a device or application compared to passwords. Biometric data can also be easier to enter compared to passwords, especially randomly generated passwords and long passwords. Biometric sensing devices can detect or image a unique physical or behavioral trait of a person and produce biometric data that can reliably identify the person. For example, a fingerprint includes a unique pattern of veins, ridges and valleys that can be imaged by a fingerprint sensor. The image of the fingerprint, or the unique characteristics of the fingerprint, is compared to previously captured reference data, such as a reference fingerprint image. The identity of the person is obtained or verified when the newly captured fingerprint image matches the reference fingerprint image.

SUMMARY

[0005] Embodiments described herein provide methods for authenticating a user with one or more biometric images and permitting the user to purchase from an online store using a biometric image or images. The terms "image" and "biometric image" are meant to encompass an image, a composite image, and other types of data that can be captured by a biometric sensing device. In one aspect, a method for completing a purchase on an online store can include a processing device determining if a biometric image matches a reference biometric image. If the biometric image matches the reference biometric image, the processing device can countersign an online account token that is associated with an account of the user on the online store with user identifier data. The countersigned online account token indicates the purchase on the online store can be completed. The countersigned token can then be transmitted to the online store, where the user is permitted to make one or more purchases on the online store based on the countersigned online account token.

[0006] In another aspect, a system can include a processing device, a biometric sensing device operatively connected to the processing device, and one or more memories operatively connected to the processing device. An online account token and user identifier data can be stored in the memory or memories. The processing device can be configured to countersign the online account token with at least some of the user identifier data when a biometric image captured by the biometric sensing device matches a reference biometric image.

[0007] In another aspect, a network communications interface can be operatively connected to the processing device. The processing device can then transmit the countersigned online account token to the online store using a network connection established with the network communications interface.

[0008] In yet another aspect, a method for authenticating a user having an account on an online store can include the online store transmitting an online account token associated with the account to an electronic device, and the online store receiving a countersigned online account token from the electronic device. The countersigned online account token can indicate the identity of the user has been authenticated based on a biometric image and can indicate the biometric image is associated with the account.

BRIEF DESCRIPTION OF THE DRAWINGS

[0009] Embodiments of the invention are better understood with reference to the following drawings. The elements of the drawings are not necessarily to scale relative to each other. Identical reference numerals have been used, where possible, to designate identical features that are common to the figures.

[0010] FIG. **1** is a perspective view of one example of an electronic device that can include, or be connected to a biometric sensing device;

[0011] FIG. **2** is an illustrative block diagram of the electronic device **100** shown in FIG. **1**;

[0012] FIG. **3** depicts an enlarged and simplified cross-sectional view of a portion of a fingerprint sensor taken along line **3-3** in FIG. **1**;

[0013] FIG. **4** is a flowchart of a method for setting up a biometric sensing device for use in online commerce;

[0014] FIG. **5** is a data flow diagram of the method shown in FIG. **4**;

[0015] FIG. **6** is a flowchart of a method for purchasing from an online store;

[0016] FIG. **7** is a data flow diagram of the method shown in FIG. **6**;

[0017] FIG. **8** is a flowchart of a method for purchasing from an online store on an electronic device with an account established after the method of FIG. **4** has been performed on the electronic device;